15114

Designed for Brilliance. Engineered for Production.

May 15, 2019

«First_Name» «Last_Name»
«Address»
«City», «State» «ZipCode»

VIA U.S. Mail and Email
«EMAIL»

Notice of Data Breach

Dear «First_Name» «Last_Name»:

We are writing to you because our investigation indicates that your personal information may have been subject to a data breach.

Upon learning of the incident, we shut down the affected account to prevent further activity and initiated an internal investigation including engaging an IT security firm to conduct a forensic analysis to provide us with more information about the event. We will provide an update to this Notice, if our investigation reveals new relevant information.

ESI, a wholly owned subsidiary of MKS Instruments, Inc., is committed to maintaining the privacy of employee information. We will continue our efforts to promote awareness of cyber-intrusions among our employees. In response to this and the increasing number of such incidents, we monitor our company's systems and adjust practices to enhance the security of sensitive information.

As part of our response to this incident, we are offering to reimburse you for eighteen months of credit and identity monitoring service through LifeLock as well as a reimbursement for a security freeze. To learn more about this service and enroll, please visit www.lifelock.com and sign up for the Ultimate Protection plan. Reimbursement request may be made by sending any receipts directly to me.

You have the right to obtain a police report. More information and a summary of additional steps you can take to protect your personal information is also enclosed. Please carefully review this information, which includes recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file, contact information for the three major credit reporting agencies and suggestions for obtaining and reviewing your credit report. If you have questions, please contact Katerina Kogan, at kogank@esi.com.

Sincerely,

Donna Knees
Director of Human Resources
Equipment & Solutions Division
MKS Instruments, Inc.

Enclosure

IDENTITY THEFT PREVENTION and PROTECTION

Monitor Your Accounts and Credit Reports, and Notify Police and the FTC of Suspicious Activity:
When you receive account statements, credit reports, and monitoring alerts, review them carefully for unauthorized activity. For example, look for accounts you did not open, unauthorized purchases, inquiries from creditors that you did not initiate, and personal information that you do not recognize, such as a home address or Social Security number. If you have concerns, call your bank, the account provider, or the credit reporting agency at the telephone number on the statement or report. If possible, place a security verification word on your accounts.

If you suspect any fraudulent activity or identity theft, promptly report it to local law enforcement authorities, your state attorney general, and/or the **Federal Trade Commission**. To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Request copies of any police or investigation reports created, as you might need to provide this information to credit reporting agencies or to supposed creditors to clear up your records.

***Obtain Free Credit Reports*:** Even if you do not find any signs of fraud on your reports, you should check your credit report regularly. There are three main credit reporting agencies: Equifax, Experian, and TransUnion. Their contact information, along with contact information for the FTC and some state agencies, are on the reverse side. Each credit reporting agency must provide you annually with a free credit report, at your request made to a single, centralized source for the reports, AnnualCreditReport.com. You are not required to order all three reports at the same time; instead, you may rotate your requests so that you can review your credit report on a regular basis. In addition, many states have laws that require the credit reporting agencies to provide you with a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

***Fraud Alert*:** You may ask the credit reporting agencies to place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three credit reporting agencies. As soon as that agency processes your fraud alert, it is supposed to notify the other two, which then also must place fraud alerts in your file. An *initial fraud alert* stays in your file for at least 90 days. An *extended alert* stays in your file for seven years. To place either of these alerts, a credit reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency.

Security Freeze: You also have the right to place a security freeze on your credit report at any of the three main credit reporting agencies. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request. If you choose to send a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail, the following information must be included when requesting a security freeze: (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to $5.00 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the agency.

Internal Revenue Service: Tax-related identity theft is when someone uses your Social Security number to file a false tax return claiming a fraudulent refund. If you received IRS correspondence indicating you may be a victim of tax-related identity theft or your e-file tax return was rejected as a duplicate, take the following steps with the IRS:

- Submit an IRS Form 14039, Identity Theft Affidavit
- Continue to file your tax return, even if you must do so by paper, and attach the Form 14039
- Watch for any follow-up correspondence from the IRS and respond quickly.

The fillable IRS Form 14039 is available at IRS.gov. Follow the instructions exactly. You can fax or mail it or submit it with your paper tax return if you have been prevented from filing because someone else has already filed a return using your SSN. You only need to file it once.

Tax Fraud Prevention

When a SSN number is compromised, it is important to notify the IRS that you may be at risk of being a future victim of identity theft. We are providing you this information to assist you in steps you should take to protect yourself from potential tax fraud. If you have not filed your federal return before February 15, 2017 you will need to do the following.

- First step is to call the IRS Identity Protection Specialized Unit at 1-800-908-4490. Select language option and then:
    - Press 2 (victim of potential identity theft)
    - Press 3 (ID Theft representative)
- Notify them that your SSN and W-2 information has been compromised and you need to confirm that no attempt of filing has been made to date. This representative can assist you with any further actions needed based on this inquiry.
- IRS provides guidance at www.identitytheft.gov

***Contact Information for the FTC and Credit Reporting Agencies*:**

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/bcp/edu/microsites/idtheft/

AnnualCreditReport.com
Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281
www.annualcreditreport.com

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian
P.O. Box 2104
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022
1-800-888-4213
www.transunion.com

***Contact Your State's Agency*:**

Massachusetts' Attorney General
Attn: Maura Healey
1 Ashburton Pl.
Boston, MA 02108
1-617-727-2200